SYSTEM AND METHODS FOR NONINTRUSIVE DATABASE SECURITY

ABSTRACT OF THE DISCLOSURE

5   Typical conventional database security scheme mechanisms are integrated in either the application or database. Maintenance of the security scheme, therefore, such as changes and modifications, impose changes to the application and/or database. Configurations of the invention employ a security filter for intercepting database streams, such as data access transactions, between an application and the a data repository, such as

10   a relational database. A security filter deployed between the application and database inspects the stream of transactions between the application and the database. The security filter, by nonintrusively interrogating the transactions, provides a content-aware capability for seamlessly and nondestructively enforcing data level security. A security policy, codifying security requirements for the users and table of the database, employs

15   rules concerning restricted data items. The filter intercepts transactions and determines if the transaction triggers rules of the security policy. If the transactions contain restricted data items, the security filter modifies the transaction to eliminate the restricted data items.